



Protección de datos mediante encriptación



INTRODUCCIÓN

En este laboratorio, se conectará a un servidor de archivos que está alojado en una instancia de Amazon EC2. Configuraré la interfaz de línea de comando (CL) de AWS Encryption en la instancia. Crearé una clave de cifrado usando AWS KMS. La clave se usará para cifrar y descifrar datos. A continuación, crearé múltiples archivos de texto que, de forma predeterminada, no están cifrados. Luego usará la clave de AWS KMS para cifrar los archivos y verlos mientras se cifran. Finalizará el laboratorio al descifrar los mismos archivos y ver los contenidos.

OBJETIVOS

- Configurar Crear una clave de cifrado de AWS KMS
- Instalar la CLI de AWS Encryption
- Cifrar datos de texto simple
- Descifrar texto cifrado.



TAREA 1

Con AWS KMS, puede crear y administrar claves criptográficas y controlar su uso a lo largo de una amplia variedad de servicios de AWS y en sus aplicaciones. AWS KMS es un servicio seguro y resiliente que usa módulos de seguridad de hardware (HSM) que están validados por el Estándar de procesamiento de información federal (FIPS) Publicación 140-2, o están en el proceso de ser validados, para proteger sus claves.

- En la consola, ingrese KMS en la barra de búsqueda y luego seleccione Key Management Service.
- Seleccione Create a key.
- En Key type, seleccione Symmetric y luego seleccione Siguiente.

The screenshot shows the AWS Management Console interface for the 'Configurar clave' (Configure key) wizard. The breadcrumb trail at the top indicates the path: KMS > Claves administradas por el cliente > Crear clave. The left sidebar lists five steps: Paso 1: Configurar clave (selected), Paso 2: Añadir etiquetas, Paso 3: Definir permisos de administración de claves, Paso 4: Definir permisos de uso de claves, and Paso 5: Revisar. The main content area is titled 'Configurar clave' and contains two sections. The first section, 'Tipo de clave' (Key type), has a link 'Ayuda para elegir' and two options: 'Simétrico' (Symmetric), which is selected with a radio button and described as 'Una única clave que se utiliza para cifrar y descifrar datos o generar y verificar códigos HMAC', and 'Asimétrico' (Asymmetric), described as 'Un par de claves públicas y privadas que se utilizan para cifrar y descifrar datos, firmar y verificar mensajes o derivar secretos compartidos'. The second section, 'Uso de claves' (Key use), also has a link 'Ayuda para elegir' and two options: 'Cifrado y descifrado' (Encrypt and decrypt), which is selected with a radio button and described as 'Utilice la clave solo para cifrar y descifrar datos', and 'Generar y verificar MAC' (Generate and verify MAC), described as 'Utilice la clave solo para generar y verificar códigos de autenticación de mensajes basados en hash (HMAC)'.



- o En la página Add labels configurar Alias y descripción. Seleccione Next.

Añadir etiquetas

Alias
Puede cambiar el alias en cualquier momento. [Más información](#)

Alias
MyKMSKey

Descripción - Opcional
Puede cambiar la descripción en cualquier momento.

Descripción
Key used to encrypt and decrypt data files.

Etiquetas - Opcional

Puede usar etiquetas para clasificar e identificar sus claves de KMS y hacer un seguimiento de los costos de AWS. Cuando agrega etiquetas a los recursos de AWS, se genera un informe de asignación de costos para cada etiqueta. [Más información](#)

Esta clave no tiene etiquetas.

- o En la página Define key administrative permissions, en la sección Key administrators, busque y seleccione la casilla para voclabs y luego seleccione Next.

Definir permisos de administración de claves

Administradores de claves (1/17)
Elija qué usuarios y roles de IAM pueden administrar esta clave a través de la API de KMS. Es posible que deba agregar permisos adicionales para que los roles o los usuarios administren la clave desde esta consola. [Más información](#)

Q voclabs X 1 coincidencias < 1 >

<input checked="" type="checkbox"/>	Nombre	Ruta	Tipo
<input checked="" type="checkbox"/>	voclabs	/	Role

Eliminación de claves

☒ Permita que los administradores de claves eliminen esta clave.

Cancelar Anterior **Siguiente**



- o En la página Define key usage, en la página This account, busque y seleccione la casilla para voclabs y luego seleccione Next. Revise la configuración y luego seleccione Finish.

Definir permisos de uso de claves

Usuarios de claves (1/17)
Seleccione los usuarios y roles de IAM que pueden utilizar la clave de KMS en operaciones criptográficas. [Más información](#)

Q voclab X 1 coincidencias < 1 >

<input checked="" type="checkbox"/>	Nombre	Ruta	Tipo
<input checked="" type="checkbox"/>	voclabs	/	Role

Otras cuentas de AWS

Especifique las cuentas de AWS que pueden usar esta clave. Los administradores de las cuentas que especifique son responsables de la administración de los permisos que autorizan a los usuarios y los roles de IAM a usar esta clave. [Más información](#)

- o Copie el enlace para MyKMSKey, que acaba de crear, y copie el valor ARN a un editor de texto.

Key Management Service (KMS)

Claves administradas de AWS
[Claves administradas por el cliente](#)

▼ Almacenes de claves personalizados
Almacenes de claves de AWS
CloudHSM
Almacenes de claves externos

Clave: b205b8bb-96fd-4c14-88d9-5b8306c1a525

Configuración general

Alias MyKMSKey	Estado Habilitada	Fecha de creación 21 ago 2024 0:07 GMT-5
ARN <code>arn:aws:kms:us-west-2:300185144499:key/b205b8bb-96fd-4c14-88d9-5b8306c1a525</code>	Descripción Key used to encrypt and decrypt data files.	Regionalidad Región única

Política de claves

Administradores de claves (1)

Elija qué usuarios y roles de IAM pueden administrar esta clave a través de la API de KMS. Es posible que necesite agregar permisos adicionales para que los roles y los usuarios puedan administrar la clave desde esta consola. [Más información](#)

Q Buscar Administradores de claves < 1 >

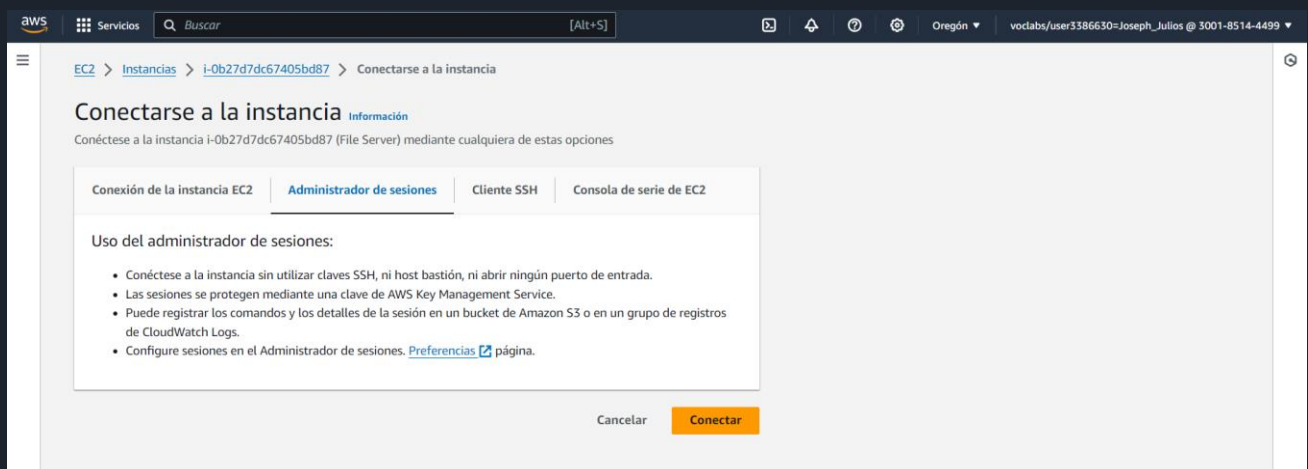
<input type="checkbox"/>	Nombre	Ruta	Tipo
--------------------------	--------	------	------



TAREA 2

Antes de que pueda cifrar y descifrar datos, debe configurar algunas cosas. Para usar su clave AWS KMS, configurará credenciales de AWS en la instancia de EC2 de File Server (Archivo de servidor). Después, instalará la CLI de AWS Encryption (aws-encryption-cli), que puede usar para cifrar y descifrar comandos.

- En la consola, ingrese EC2 en la barra de búsqueda y luego seleccione EC2.
- En la lista Instances, seleccione la casilla a su lado para la instancia de File Server y luego seleccione Connect.
- En la pestaña Session Manager, elija Connect.



- Para cambiar el directorio principal y crear el archivo de credenciales de AWS, ejecutar aws configure.



- Cuando se le solicite, configure los siguientes ajustes.

```
ID de sesión: user3386630=Joseph_Julios-          ID de instancia: i-0b27d7dc67405bd87
zh6d6ggsylhybsgimbyjl6nxjq
```

```
sh-4.2$ cd ~
sh-4.2$ aws configure
AWS Access Key ID [None]: 1
AWS Secret Access Key [None]: 1
Default region name [None]: us-west-2
```

- Navegue hasta la página de la consola de Vocareum y seleccione el botón AWS Details.
- Junto a AWS CLI, seleccione Show.
- Copie y pegue el bloque de código, que comienza con [default] (predeterminado), en un editor de texto.
- Vuelva a la pestaña del navegador en la que inició sesión en el Servidor de archivos.
- Ejecutar `vi ~/.aws/credentials` Para abrir el archivo de credenciales de AWS.
- Vuelva a la pestaña del navegador en la que inició sesión en el Servidor de archivos.
- Pegue el bloque de código que copió de Vocareum.

```
ID de sesión: user3386630=Joseph_Julios-          ID de instancia: i-0b27d7dc67405bd87
zh6d6ggsylhybsgimbyjl6nxjq
```

Terminar

```
aws_access_key_id=ASIAULZDNZSEXTJ4Q6HA
aws_secret_access_key=ecOkeYnJaOUKtNTXfCw/RxXN0U0xo3lZGMW1Y7qR
aws_session_token=IqoJb3JpZ2luX2VjBGUaCXVzLWVlc3QlMlJlMEYCIQDyOjG1dyhLi4DTV4twjCw5N5ldyC05bFQDSCSstU4bimQ1hALnx4Qet4vzAAPuWk/RhC8HZPYNLfUpM1o6YyLtUnGK/KqcCG4QABoMMzAwMTg1
MTQ0NDk5IgxMnO2KAZXXjHlqWgroghARmNOMhNjDPiBev2Mzi+/8J/sFG4W2GEUVPSPMoRVdguKVKkCTBp4DDys6KL5UkjEd3roYfH5XIM3tSs4lEtnQs9ueEaeOUY6meEVs1By3NohGT9W8RktJ9FM1Snyu1OUOWT7D3N5ug5V
L/84RHen5DlrcAzr7LZujKFYwCRwX//s1Xlr4nb3wj63JvBh1V0/aP0upauYZigvc4li+8Rj8dFdRxx+6RVczgvHMFirjSGhn3eqWD1ZDEw42RhsdEXU+tUSoNahhAZg9LDmeR3iBr6UwCamD1MHM1+uu7d8U5wtg7fWjyy8
ghxIx0rkmGeHr19VaTj8/krvHn6jgG1j2VEFVzCb6Zw2BjgcARTCaFp2XHD9Vvca/ci3omTXhjKri7GZWrthfhojVrv6Cd9drlThpraP8KIHXEWXzDj1+z3VcEkgu3/9gaqladPREW2sto8U2AT6jQrV0yrn1Z/JRL8TaybRL
WqTwGo9IrGd4d5DoCCIPuKdyB0ez8se23laICgSMUVT2E/xDhDcWHRBI6ogFFiKVMH0AR81Lzuffsfpy/9x8d84Q==
```

- Para guardar y cerrar el archivo, presione Escape, escriba `:wq` y luego presione Intro.
- Ejecutar `cat ~/.aws/credentials` para ver los contenidos actualizados del archivo.

```
sh-4.2$ cat ~/.aws/credentials
aws_access_key_id=ASIAULZDNZSEXTJ4Q6HA
aws_secret_access_key=ecOkeYnJaOUKtNTXfCw/RxXN0U0xo3lZGMW1Y7qR
aws_session_token=IqoJb3JpZ2luX2VjBGUaCXVzLWVlc3QlMlJlMEYCIQDyOjG1dyhLi4DTV4twjCw5N5ldyC05bFQDSCSstU4bimQ1hALnx4Qet4vzAAPuWk/RhC8HZPYNLfUpM1o6YyLtUnGK/KqcCG4QABoMMzAwMTg1
MTQ0NDk5IgxMnO2KAZXXjHlqWgroghARmNOMhNjDPiBev2Mzi+/8J/sFG4W2GEUVPSPMoRVdguKVKkCTBp4DDys6KL5UkjEd3roYfH5XIM3tSs4lEtnQs9ueEaeOUY6meEVs1By3NohGT9W8RktJ9FM1Snyu1OUOWT7D3N5ug5V
L/84RHen5DlrcAzr7LZujKFYwCRwX//s1Xlr4nb3wj63JvBh1V0/aP0upauYZigvc4li+8Rj8dFdRxx+6RVczgvHMFirjSGhn3eqWD1ZDEw42RhsdEXU+tUSoNahhAZg9LDmeR3iBr6UwCamD1MHM1+uu7d8U5wtg7fWjyy8
ghxIx0rkmGeHr19VaTj8/krvHn6jgG1j2VEFVzCb6Zw2BjgcARTCaFp2XHD9Vvca/ci3omTXhjKri7GZWrthfhojVrv6Cd9drlThpraP8KIHXEWXzDj1+z3VcEkgu3/9gaqladPREW2sto8U2AT6jQrV0yrn1Z/JRL8TaybRL
WqTwGo9IrGd4d5DoCCIPuKdyB0ez8se23laICgSMUVT2E/xDhDcWHRBI6ogFFiKVMH0AR81Lzuffsfpy/9x8d84Q==
sh-4.2$
```



TAREA 3

En esta tarea, creará un archivo de texto con información confidencial ficticia. Luego, usará el cifrado para asegurar los contenidos del archivo. Luego, descifrará los datos y verá los contenidos del archivo.

- Crear un archivo de texto.
- Ver los contenidos del archivo secret1.txt.

```
ID de sesión: user3386630=Joseph_Julios-          ID de instancia: i-0b27d7dc67405bd87
zh6d6ggsylhybsgimbyjl6nxjq

sh-4.2$ touch secret1.txt secret2.txt secret3.txt
sh-4.2$ echo 'TOP SECRET 1!!!!' > secret1.txt
sh-4.2$ cat secret1.txt
TOP SECRET 1!!!!
sh-4.2$
```

- Crear un directorio en el que crear el archivo cifrado.
- Ejecutar `keyArn=(KMS ARN)` en un editor de texto, reemplace `(KMS ARN)` con el AWS KMS ARN que copió en la tarea 1.
- Ejecute el comando actualizado en el terminal del Servidor de archivos.

```
ID de sesión: user3386630=Joseph_Julios-          ID de instancia: i-0b27d7dc67405bd87
zh6d6ggsylhybsgimbyjl6nxjq

sh-4.2$ mkdir output
sh-4.2$ keyArn=(KMS ARN)
sh-4.2$ keyArn=arn:aws:kms:us-west-2:300185144499:key/b205b8bb-96fd-4c14-88d9-5b8306c1a525
sh-4.2$
```




- Cifrar el archivo secret1.txt.

ID de sesión: user3386630=Joseph_Julios-
zh6d6ggsylhybsgimbyjl6nxjq

ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ aws-encryption-cli --encrypt \  
> --input secret1.txt \  
> --wrapping-keys key=$keyArn \  
> --metadata-output ~/metadata \  
> --encryption-context purpose=test \  
> --commitment-policy require-encrypt-require-decrypt \  
> --output ~/output/.  
sh-4.2$
```

- Determinar si el comando se realizó correctamente.

ID de sesión: user3386630=Joseph_Julios-
zh6d6ggsylhybsgimbyjl6nxjq

ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ echo $?  
0  
sh-4.2$
```

- Ver la ubicación del archivo recién cifrado.

ID de sesión: user3386630=Joseph_Julios-
zh6d6ggsylhybsgimbyjl6nxjq

ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ ls output  
secret1.txt.encrypted  
sh-4.2$
```

- Ver los contenidos del archivo recién cifrado.

ID de sesión: user3386630=Joseph_Julios-
zh6d6ggsylhybsgimbyjl6nxjq

ID de instancia: i-0b27d7dc67405bd87

Terminar

```
sh-4.2$ cd output  
sh-4.2$ cat secret1.txt.encrypted  
x. W0Z...aws-crypto-public-keyDAsU3kl7P4wHRSIWD0y0LnI2tZjv1+GqPyimVh12xdU74AUGLzMNJ5FcMioJIV2XGqQ==purposetestaws-kmsKarn:aws:kms:us-west-2:300185144  
0oOm0hy/...e,0bb-96fd-4c14-88d9-5b8306c1a525...xEl8...)*m01  
7k...Fm)...Nc...X...  
...gOel...x9...m...A...Lc...t8...X.../...h-4.2$
```



- Descifrar el archivo.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq

ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ aws-encryption-cli --decrypt \  
> --input secret1.txt.encrypted \  
> --wrapping-keys key=$keyArn \  
> --commitment-policy require-encrypt-require-decrypt \  
> --encryption-context purpose=test \  
> --metadata-output ~/metadata \  
> --max-encrypted-data-keys 1 \  
> --buffer \  
> --output .  
sh-4.2$
```

- Ver la ubicación del nuevo archivo.
- Ver los contenidos del archivo descifrado.

ID de sesión: user3386630=Joseph_Julios-zh6d6ggsylhybsgimbyjl6nxjq

ID de instancia: i-0b27d7dc67405bd87

```
sh-4.2$ ls  
secret1.txt.encrypted  secret1.txt.encrypted.decrypted  
sh-4.2$ cat secret1.txt.encrypted.decrypted  
TOP SECRET 1!!!  
sh-4.2$ █
```